doi: 10.3969/j.issn.1671-1122.2012.02.011

震网病毒分析与防范

蒲石，陈周国，祝世雄

（中国电子科技集团公司第三十研究所保密通信重点实验室，四川成都 610041）

摘 要： 近年来随着网络技术的发展，网络攻击发生频繁，并逐步从传统意义上的虚拟空间扩展到工业控制系统中，直接威胁着国家基础设施的信息安全。震网病毒是第一个直接破坏现实世界中工业控制网（SCADA）的恶意代码。文章通过分析震网病毒对SCADA网络的攻击过程和关键步骤，提出对工业控制网络的安全防护建议。

关键词： 网络安全；震网病毒；SCADA网络

中图分类号： TP393.08 **文献标识码：** A **文章编号：** 1671-1122（2012）02-0040-04

Analysis and Protection of Stuxnet Virus

PU Shi, CHEN Zhou-guo, ZHU Shi-xiong

(The 30th Research Institute of China Electronics Technology Group Corporation

Science and Technology on Communication Security Laboratory, Chengdu Sichuan 610041, *China)*

Abstract: With the development of technologies of network, network attacks have become direct threats to the security of national infrastructure frequently, from virtual space to the real industry control networks. Stuxnet Virus was the first malicious code to damage the industry control system in the world. This paper analyses the key progress and steps of the attack to SCADA network and makes suggestions to security protection of industry control network.

Key words: network security; stuxnet virus; SCADA network

1 震网事件

2010年9月24日，伊朗核设施曝出Stuxnet病毒（国内译“震网”）攻击，导致其核设施不能正常运行。据推测，可能是负责建设布舍尔电站的俄罗斯工程技术人员所使用的U盘是本次病毒传播的重要渠道。与传统的电脑病毒相比，震网病毒不会通过窃取个人隐私信息牟利，而是一种直接破坏现实世界中工业基础设施的恶意代码，由于其攻击对象是国家重要基础设施，因此被一些专家定性为全球首个投入实战舞台的“网络武器”。为此，美国国土安全部已成立专门机构应对震网病毒。据赛门铁克公司的统计，目前全球已有约45000个网络被该病毒感染。

2 震网病毒机理

震网病毒主要通过U盘的方式传播，针对微软操作系统中的MS10-046漏洞（Lnk文件漏洞）、MS10-061（打印服务漏洞）、MS08-067等多种漏洞使用伪造的数字签名，利用一套完整的入侵传播流程，突破工业专用局域网的物理限制，对西门子的SCADA软件进行特定攻击。

震网病毒传播的过程是首先感染外部主机，然后感染U盘，利用快捷方式文件解析漏洞，传播到内部网络，在内网中，通过快捷方式解析漏洞、RPC远程执行漏洞、打印机后台程序服务漏洞，实现联网主机之间的传播；最后抵达安装了WinCC软件的主机，展开攻击。震网病毒采取多种手段进行渗透和传播，具体感染过程如图1所示[1]。

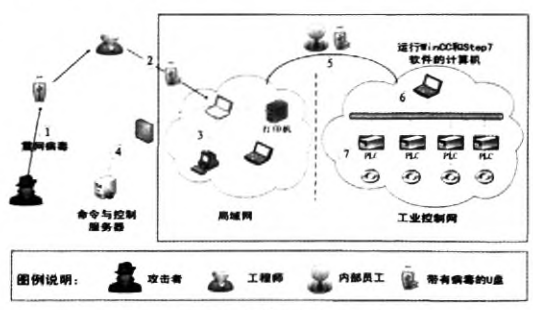

图1 震网病毒传播过程示意图

收稿时间： 2011-12-18

作者简介： 蒲石（1982-），男，四川，工程师，硕士，主要研究方向：网络安全；陈周国（1980-），男，四川，工程师，硕士，主要研究方向：信息安全；祝世雄（1965-），男，重庆，研究员，硕士，主要研究方向：密码学、信息安全体系及保密通信技术研究

1）通过感染病毒的USB驱动器感染目标系统中的某台机器；2）通过感染病毒的USB驱动器感染目标系统中的局域网；3）在感染了某台Windows工作机器后，震网病毒尝试在局域网中传播；4）震网病毒尝试与外网的命令和控制（Command和Control，C&C）服务器通信；5）震网病毒感染工业网中装有WinCC软件的工作站；6)当被感染的工作站连接到PLC时，震网病毒根据PLC（Programmable Logic Controller）的情况，部署恶意代码；7）恶意代码向设备发送特定的指令。

震网病毒一旦安装在计算机上，它利用西门子的默认密码去获得访问系统的权限，这些系统上运行着Simatic Step7和WinCC程序，因为这些程序可以控制和修改运行在可编程逻辑控制器PLC上的代码，而PLC控制着设备的运行状态（例如机器转速等），震网病毒最终的攻击目标就是PLC。

3 震网病毒执行分析

震网病毒与常见的病毒类似，分为传播、安装和攻击执行阶段。我们按照震网病毒传播、安装及执行阶段对其进行深入剖析。

3.1 传播阶段

震网病毒包含6个文件：4个恶意的快捷方式和两个可执行临时文件。当新的驱动器（USB闪存）插入计算机的时候，震网病毒会得到通知，并向闪存驱动器写入6个文件，6个文件分别为：

1）4个快捷方式：

Copy of Shortcut to.lnk;

Copy of Copy of Shortcut to.lnk;

Copy of Copy of Copy of Shortcut to.lnk;

Copy of Copy of Copy of Copy of Shortcut to.lnk。

2）2个可执行文件（DLL文件）：

~WTR4141.tmp;

~WTR4132.tmp。

震网病毒使用Rootkit技术隐藏文件，用户一般看不到上述6个文件。4个恶意的快捷方式作用基本相同，之所以要使用4个快捷方式文件，就是为了确保震网病毒利用的漏洞，能够兼容所有版本的Windows操作系统。恶意的快捷方式使用的是Windows Shell LNK漏洞（MS-10-046），但这个漏洞不是缓冲区溢出漏洞，只是由于Windows对于Lnk文件，载入图标的错误方式，从而产生了漏洞。

震网病毒的执行不需人工干预，它利用Windows Explorer Shell（Shell32.dll）快捷方式解析代码中的零天漏洞（目前，微软已经于2010年8月发布了该漏洞补丁KB2286198），用户需要做的仅仅是打开含有震网文件的目录。图2显示的是震网病毒传播的执行流程。

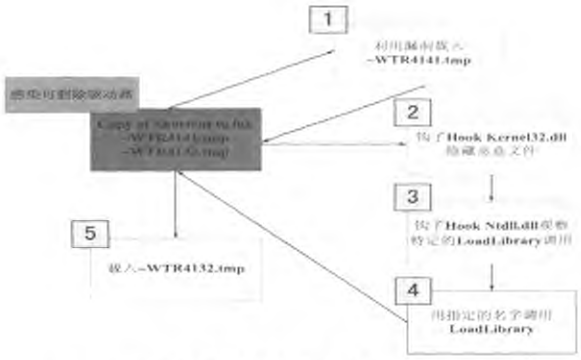

图2 震网病毒传播的执行流程

1)~WTR4141.TMP文件是个DLL文件，它由Lnk漏洞载入，用于载入~WTR4132.TMP文件。这个文件不仅用于载入震网病毒的主要部分（~WTR4132.TMP），而且工作在用户模式的Rootkit下，在闪存中隐藏震网文件。

2）~WTR4141.TMP文件hook kernel32.dll中的文件管理API，修改主进程（Explorer.exe）的入口表，这些函数调用原始Windows函数的API，修改它们的输出，用于隐藏震网文件，达到隐藏恶意文件的目的。

3）hook Ntdll.dll文件观察LoadLibrary函数调用。

4）用指定的名字LoadLibrary函数。

5）载入~WTR4132.TMP文件，实施进一步攻击。

3.2 安装阶段

一般来说，恶意软件的安装需要提升系统控制权限，震网病毒利用两个零日安全漏洞来提升权限。首先检查配置数据是否是最近和正确的，然后检查是否是管理员权限。如果它不运行在管理员级别，使用两个零日漏洞（Win32K.sys Keyboard Layout漏洞和Windows Task Scheduler漏洞）中的一个，提升权限，并使程序运行在管理员级别。这两个漏洞存在于所有的Windows系统中。第一个能够提升旧版本系统Windows 2000和XP)的权限；第二个能够能够提升新版本系统Windows Vista、7和2008）的漏洞[2]。

当一切环境准备就绪，病毒从一个进程注入到另一个进程，从而安装自己。注入时，它搜索安装在机器上的反病毒程序。根据杀毒软件的类别，震网病毒自行选取注入的进程[3]，如果没有安装杀毒软件，它会注入lsass.exe。

震网病毒会在Windows目录安装6个文件，分别是4个加密文件和两个驱动文件。病毒将设备驱动安装在注册表中，并确保每次计算机启动时驱动都会运行[4]。文件的典型形式如下：

C:\WINDOWS\inf\oem7A.PNF

C:\WINDOWS\inf\oem6C.PNF

C:\WINDOWS\inf\mdmcpq3.PNF

C:\WINDOWS\inf\mdmeric3.PNF

C:\WINDOWS\system32\Drivers\mrxnet.sys

C:\WINDOWS\system32\Drivers\mrxcls.sys

如果我们查看注册表，会看到如图 3 所示的信息。

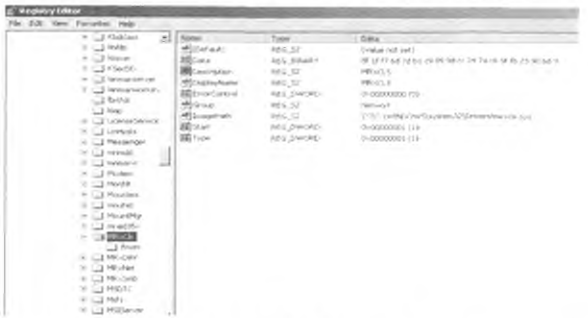

图3 在注册表中查看信息

通过工具 Process Explorer 比较进程前后被注入的情况。从图 4 中可以看到，工具检测到两个新注册的设备驱动 Mrxnet.sys 和 Mrxcls.sys。

图4 新注册了两个设备驱动

通过 Process Explorer 工具，Mrxcls.sys 和 Mrxnet.sys 两个驱动文件在载入的驱动列表中是可见的。同时可知驱动文件来自微软，而数字签名来自 Realtek[5]，如图 5 所示。

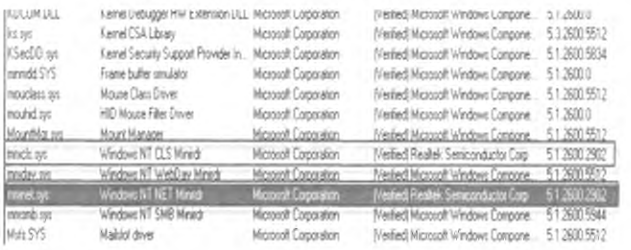

图5 数字签名信息

使用逆向工程技术对内核模式的 Rootkit 程序 MRxNet 逆向，其结果如图 6 所示。

```
NTSTATUS DriverEntry(IN PDRIVER_OBJECT pDriverObject, IN PUNICODE_STRING theRegistryPath )
{
    int i;
    NTSTATUS status;
    DriverObject=pDriverObject;
    status=IoCreateDevice(DriverObject, sizeof(_DEVICE_EXTENSION),0,FILE_DEVICE_DISK_FILE_
    if (status!=STATUS_SUCCESS){
        IoDeleteDevice(DeviceObject);
        return 0;
    }
    SetZero(DeviceObject->DeviceExtension,0);
    for(i = 0; i <= IRP_MJ_MAXIMUM_FUNCTION; i++ )
    {
      DriverObject->MajorFunction[i] = IRPDispatchRoutine;
    }
    DriverObject->MajorFunction[IRP_MJ_FILE_SYSTEM_CONTROL] = OnFileSystemControl;
    DriverObject->MajorFunction[IRP_MJ_DIRECTORY_CONTROL] = OnDirectoryControl;
```

图6 MRxNet程序逆向的结果

MRxNet 的主要目的是借助 Windows 创建的函数，修改任意驱动的输出，如图 7 所示。

```
);
PrevIrpStack = (ULONG)Irp->Tail.Overlay.CurrentStackLocation -
PrevIrpStack->Control=0;
PrevIrpStack->Context = Buff;
PrevIrpStack->CompletionRoutine = FileControlCompletionRoutine;
PrevIrpStack->Control=0xE0;
return 1;
```

图7 修改驱动的输出

Mrxnet.sys 是一个 Rootkit 程序，用来隐藏文件。当系统启动时，Mrxcls.sys 启动恶意软件。由于有知名硬件公司合法的数字签名，人们不会太注意这些文件。

通过微软公司的工具 Process Explorer, Autoruns 和 VMMap 可以调查病毒注入系统后的情况。Autoruns 揭示了震网病毒的核心，两个驱动文件 Mrxcls.sys 和 Mrxnet.sys。通过证实，禁用这两个驱动，然后重启，是让震网病毒失效的必要条件。通过工具分析，我们可以知道，震网病毒将代码注入到了系统的许多进程中，并创建了运行系统可执行文件的进程，作为攻击载荷数据的宿主。

一旦恶意软件安装在 Windows 系统上，一旦它安装了 RPC 服务器，此时便具有了许多功能，它可以作为网络中的一部分工作，也可以与局域网中被感染的系统交互信息。

震网病毒通过使用 RPC 服务，借助 P2P 的方式，使被攻克的系统载入恶意代码到内存并执行。它试图与外界的命令和控制（Command 和 Control）服务器进行通信。

3.3 攻击阶段

震网病毒攻击的核心目标是工业控制网的 PLC，因为 PLC 直接控制着设备的运转状态。一旦 Windows 系统被攻克（第一阶段）和恶意软件被安装（第二阶段），那么第三个阶段就是攻击了。恶意软件搜索特定的程序，访问工业控制系统，其选择的攻击对象是目标系统的开发工具如 Step7 和 WinCC。这两个工具分别用来开发在 PLC 系统上的程序，功能监视和函数检查等功能。如果底层系统不连接互联网，这些开发工具可能是接触底层系统的唯一入口。

震网病毒查询下列两个注册表的键值来判断主机中是否安装 WinCC 系统[6]，如图 8 所示：

HKLM\SOFTWARE\SIEMENS\WinCC\Setup

HKLM\SOFTWARE\SIEMENS\STEP7

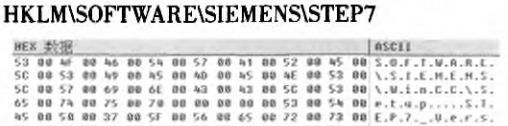

图8 查询注册表，判断系统是否安装WinCC

一旦发现 WinCC 系统，就利用 WinCC 软件的两个漏洞展开攻击。1）WinCC 系统中存在一个硬编码漏洞，保存了访问数据库的默认账户名和密码，震网病毒利用这一漏洞尝试访问该系统的 SQL 数据库，如图 9 所示；2）在 WinCC 需要

```
文本字串
declare @t varchar(4000), @e int, @f int if exists (select text from dbo
declare @t varchar(4000), @e int, @f int if exists (select * from dbo.sy
use master
.mdf
select name from master..sysdatabases where filename like n'%s'
.mdf
.ldf
exec master..sp_attach_db 'wincc_svr',n'%s',n'%s'
exec master..sp_detach_db 'wincc_svr'
use wincc_svr
exec master..sp_detach_db 'wincc_svr'
.mdf
.ldf
 ((select top 1 1 from mcpvreadvarpercon)='1') --cc-sp
x
@
.mdf
.mdf
vector<t> too long
2wsxcder
winccconnect
master
.\wincc
sqloledb
provider='%s';data source=%s;initial catalog='%s';user id='%s';password=
```

图9 查询WinCC 的数据库

使用的Step7 工程中，在打开工程文件时，存在 DLL 加载策略上的缺陷，从而导致出现一种类似于“DLL 预加载攻击”的利用方式。最终，震网病毒通过替换 Step7 软件中的 s7otbxdx.dll，而将原来的同名文件修改为 s7otbxsx.dll，并对这个文件的导出函数进行一次封装，从而实现对一些查询、读取函数的 Hook。s70tbxdx.dll 是 Simatic 软件套装中一个共享链接库，它用来与 Simatic 系列的 PLC 通信。通常，开发者使用 STL 或 SCL 语言为设备编程。程序通常被编译为一种称为 MC7 的汇编代码，被 PLC 载入。正常情况下，WinCC 的 Step 7 软件使用库文件 s7otbxdx.dll 来和 PLC 通信。

将共享库函数文件 s70tbxdx.dll 重命名为 s70tbxsx.dll，恶意软件伪装成合法的 s70tbxdx.dll 文件，能够拦截对原始库函数 s70tbxdx.dll 的调用，并任意操作调用。大多数对函数 s70tbxdx.dll 的调用都被直接发送给被替换了的函数 s70tbxsx.dll。如图 10 所示，原始库函数 s70tbxdx.dll 的大小为 1175552 字节，而恶意库函数大小为 298000 字节。

Name	Ext	Size
S7OTBEMK	DLL	86 016
S7otbldx	dll	98 357
s7otbxDx	dll	298 000
s7otbxdx ORIGINAL	dll	1 175 552
s7otbxsx	dll	1 175 552
s7owpstx	dll	176 128

图10 原始库函数s70tbxdx.dll和恶意库函数s70tbxDx.dll的比较

系统遭受攻击后，Step 7 软件调用被替代的 s70tbxdx.dll 和 PLC 通信，于是震网病毒可以拦截任何来自其他软件访问 PLC 的命令，从而实施侦察攻击。具体过程如图 11 和图 12 所示。

图11 Step7控制软件可以控制PLC的运行状态

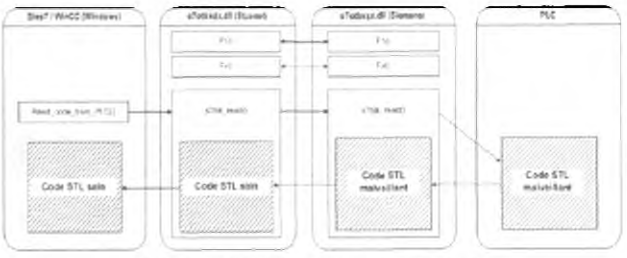

图12 震网病毒拦截WinCC和PLC的通信

4 结束语

震网病毒震动了世界工业界，破灭了专用网络、专用系统固有的安全基础，我们应高度警惕物理隔离的专业系统的网络安全。

4.1 增加漏洞及其挖掘技术研究

“震网”病毒攻击事件后，工业级的控制软件的安全逐步得到大家的重视，通过挖掘发现存在大量的零日漏洞。例如 2011 年 3 月，US-CERT 控制系统安全小组就发现，在西门子等公司的多款 SCADA 网络产品中存在多种漏洞。SCADA 系统被广泛应用在石油、电力、水利等工业领域，承担着数据采集、监视控制等各种任务，是目前应用最广、技术发展最成熟的工业控制系统。因此需要大力研究 SCADA 系统漏洞及其漏洞挖掘技术，只有充分认识这些漏洞及其挖掘技术才能防范于未然，甚至为我所用，以其人之道还治其人之身。

4.2 加大信息网络安全管理

加强国家信息网络安全管理，从内网和外方两个方面协调进行，对重点信息网络应采用自主可控的信息安全设备及技术。

4.3 建立重要网络应急响应机制

由于网络安全技术发展日新月异，需要建立重要信息基础设施的应急响应机制，实现对重要目标或系统的监测、防护和应急处理，采取技术手段实现追踪定位、灾害恢复和攻击反制。

同时，建立一种类似西方国家实战演习的工作方式，定期进行内外网的网络安全演练，发现技术、制度上的薄弱环节，及时应对。● （责编 程斌）

参考文献：

[1] David Helan. Stuxnet: analysis,myths and realities [J].Actusecu 27,2010:14-23.

[2] Amr Thabet.Stuxnet_Malware_Analysis_Paper[J].Freelancer Malware Researcher，2010: 3-28.

[3] Nicolas Falliere, Liam O Murchu, Eric Chien.W32.Stuxnet Dossier[R]. Symantec company，2011.16-38.

[4] Matrosov, Rodionov.Stuxnet_Under_the_Microscope 1.3[R]. ESET Company，2010.24-65，

[5] Mark Russinovich. Analyzing a Stuxnet Infection with the Sysinternals Tool[EB/OL]. http://blogs.technet.com/b/markrussinovich/archive/2011/03/30/3416253.aspx，2010.

[6] 安天实验室．对 Stuxnet 蠕虫攻击工业控制系统事件的综合报告[R]. 安全实验室，2010.4-11.